Defensive Islanding to Enhance the Resilience of Distribution Systems against Cyber-induced Failures

Michael Abdelmalak[1], Mukesh Gautam[1], Jitendra Thapa[1], Eliza Hotchkiss[2], and Mohammed Benidris[1],
[1]Department of Electrical and Biomedical Engineering, University of Nevada-Reno, Reno, NV 89557, USA
[2]National Renewable Energy Laboratory, Golden, CO 80401, USA
Emails: {mabdelmalak, mukesh.gautam, jitendrathapa}@nevada.unr.edu,
eliza.hotchkiss@nrel.gov, mbenidris@unr.edu

***Abstract*—The extensive integration of communication, computation, and control technologies into cyber-physical power systems (CPPSs) has increased the vulnerabilities of CPPSs to cyberattacks. This calls for developing solutions that assess and reduce the impacts of cyber-induced failures on CPPSs. This paper proposes a defensive islanding strategy to isolate impacted parts of the CPPS and form self-sufficient islanded grids with an objective of minimum load curtailment. The defensive islanding aims to split a power system into smaller grids to improve its resilience against a potential extreme event. A clustering approach that leverages the hierarchical spectral clustering method is utilized for the optimal defensive islanding. The proposed approach captures the fragility behavior and loading conditions of power system components due to cyber-induced failures. A graphical-based coupling framework is used to map the impacts of cyber failures into operation of power system components. The proposed method is demonstrated on a modified 33-node distribution feeder system integrated with distributed energy resources. The amount of load curtailment and radiality constraints have been used to evaluate the performance of the proposed clustering strategies. The results show the capability of the proposed algorithm to create islands considering the cyber-induced failures for enhanced resilience.**

***Index Terms*—Cyber-induced failures, cyber-physical system, islanding, microgrid, resilience.**

I. Introduction

Modern power systems are inundated with the rapid deployment of information, computation, and communication technologies. The deep coupling between information and power system through various communication means has transformed power systems into cyber-physical power systems (CPPSs) [1], [2]. Though this integration has enabled diverse applications of automation and control for enhanced performance of CPPS, vulnerabilities of power systems to cyber failures and cyberattacks have increased dramatically [3], [4], which can lead to major blackouts [5]. For example, the cyberattack on the Ukrainian power grid on December 2015 resulted in a blackout that affected 225,000 residents [6]. In CPPSs, the impact of cyber-induced failures have gained noticeable interest in reliability-based and resilience-based studies [7]. Other studies have focused on detection and mitigation techniques of cyberattacks [8]. However, the role of islanding techniques to enhance resilience of CPPS against cyber-induced failures is still under investigation. Clustering approaches, which are effective approaches for determining optimal islanding, rely mainly on the properties of the physical layer solely giving less interest to coupling behavior of cyber-layers. Therefore, implementing a resilience-based enhancement strategy due to cyber-induced failures has become important than ever.

Several methods have been proposed to enhance the resilience of power systems using islanding and microgrid formation strategies. A spectral clustering algorithm has been employed to determine optimal network partitions under tight potential $N-k$ (i.e., $k>1$) contingencies [9]. A risk-based defensive islanding approach has been studied in [10] to reduce the impact of cascading failures on transmission systems for enhanced resilience against hurricanes. In [11], a multi-layer constrained clustering technique has been investigated to split a power system into islands while minimizing power disruptions. Also, a clustering approach has been integrated with frequency measurements of inverter-based resources to create islanded grids based on transient responses of renewable energy resources [12]. In [13], a resilience-based microgrid formation framework has been proposed to enhance the restoration of critical loads in both radial and meshed networks. Most of these studies have focused on transmission level due their highly meshed topology. Despite the significant contributions of these methods to enhance islanding strategies, impacts of cyber-induced failures on microgrid formation of distribution CPPSs require further investigation.

The impact of cyber-induced failures on the operational performance of CPPS has gained significant interest. A CPPS model representing the IEEE 118-bus system integrated with a communication network has been used to assess the impact of malware-induced cyberattacks [14]. An exploration approach to identify the most vulnerable components to malicious external attacks in nuclear power plants has been studied in [15]. A resilience-based mechanism to improve the recovery rate of communication links impacted by a cyberattack has also been proposed in [16]. A defensive enhancement scheme has been proposed in [17] to reduce the likelihood of cyber-induced failures in waste water treatment systems, as seen in Oldsmar, Florida in February 2021 [18] and San Francisco, California in January 2021 [19]. In [20], the impact of cyber-induced depended failures on composite power system reliability has been investigated. Also, a CPPS model has been proposed in [21] to capture the propagation of cyber failures into distribution power systems for reliability evaluation. The role of cyber-induced failures in islanding strategies is still underdeveloped. Also, most of these studies have focused on performance evaluation against cyber-induced failures rather than defensive islanding of CPPS. Therefore, an islanding method that captures the correlation between physical operating conditions and cyber fragility behavior in CPPSs is required for enhanced resilience.

This paper proposes a clustering approach to split distribution systems into microgrids based on assessing their vulnerabilities to cyber-induced failures. The proposed algorithm leverages the hierarchical spectral clustering approach based on graph network representation of the cyber-physical system under study. The clustering approach isolates the distribution system at the most vulnerable components yielding a defensive preparedness scheme for enhanced resilience. The potential impacts of a cyber failure scenario is reflected on the power system using a graphical-based coupling framework between cyber layers and physical layers. The list of vulnerable components is obtained by integrating the steady-state parameters (power flows) of the physical system with the fragility behavior (failure probability) of cyber components. The minimal amount of load curtailment and radiality constraints are used to validate the efficiency of the obtained islands for enhanced restoration performance. The proposed algorithm is tested on a modified 33-node system integrated with distributed energy resources.

The rest of the paper is organized as follows: Section II describes the defensive islanding approach for CPPS. Section III explains the hierarchical spectral clustering method and the clustering evaluation criteria. Section IV illustrates the implementation procedures on the 33-node distribution feeder and discusses the results. Section V provides some concluding remarks.

II. Cyber Resilience-based Defensive Islanding

This section describes the representation of a cyber-physical power system as a graph network. Also, it illustrates a defensive islanding approach using graphical clustering. Finally, a few weighting functions are proposed to capture both the physical and cyber features for proper clustering.

A. Graphical Representation of Cyber-Physical Power System

CPPSs are usually divided into of a physical layer representing the power grid and a cyber layer including communication and computation systems. According to complex network theory, both physical and cyber layers can be represented as graph networks [2]. A physical power system is represented by a undirected graph $\mathcal{G}_\mathcal{P} = (\mathcal{N}_\mathcal{P}, \mathcal{E}_\mathcal{P})$, where $\mathcal{N}_\mathcal{P}$ is a set of vertices corresponds to buses or nodes in the power system and $\mathcal{E}_\mathcal{P}$ is a set of edges referring to transmission line segments or transformers. Following the same convention, the cyber layer can be represented as a undirected graph $\mathcal{G}_\mathcal{C} = (\mathcal{N}_\mathcal{C}, \mathcal{E}_\mathcal{C})$, where $\mathcal{N}_\mathcal{C}$ is a set of vertices that correspond to communication routers and control centers in the cyber system and $\mathcal{E}_\mathcal{C}$ is a set of edges representing the communication channels between the information nodes.

The coupling between the information equipment and power system components shows the strong inter-dependency between the cyber and physical layers. In a conventional CPPS, the communication network is responsible for transferring measurements from power system sensors and sending decision control signals to power system actuators [2]. Various studies have been conducted to present a coupling model of the physical and cyber layers [7], [21], [22]; however, such coupling differs based on the system under study, the level of interaction among different layers, and the scope of the study. This paper focuses on propagating the impact of cyber-induced failures into a power system. The presented coupling model between communication and physical layers is adopted from [23] and summarized as follows. A node-switch incidence matrix $A^{ns} \in \mathbb{R}^{\mathcal{N}_\mathcal{P} \times \mathcal{N}_\mathcal{C}}$ that represents the communication channel between a physical node and its terminal in the cyber layer can be constructed as follows.

$$a^{ns}_{i,j} = \begin{cases} 1 & \text{if node } i \text{ is connected to switch } j \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

Also, a branch-switch incidence matrix $A^{bs} \in \mathbb{R}^{\mathcal{E}_\mathcal{P} \times \mathcal{N}_\mathcal{C}}$ describing the relationship between a physical edge and its assigned communication router can be formulated as follows.

$$a^{bs}_{i,j} = \begin{cases} 1 & \text{if branch } i \text{ is connected to switch } j \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

Finally, a switch-switch incidence matrix $A^{ss} \in \mathbb{R}^{\mathcal{N}_\mathcal{C} \times \mathcal{N}_\mathcal{C}}$ can be used to describe the existing communication topology, such as star, ring, or meshed, and can be formed as follows.

$$a^{ss}_{i,j} = \begin{cases} 1 & \text{if switch } i \text{ is connected to switch } j \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

B. Defensive Islanding

Defensive islanding aims to split a power system into smaller independent grids and isolate the vulnerable components based on constrained clustering. The defensive islanding approach provides a proactive strategy to exclude the vulnerable system components for enhanced resilience operation. Existing islanding approaches rely mainly on the topology and loading conditions of the physical electric power system [10], [24]. However, the integration of communication and cyber components introduces further challenges on clustering a CPPS [23]. For instance, during an extreme weather event, the communication channels connecting the power system components, such as circuit breakers, and tie-switches, to the main control center can be compromised. Though power components can still operate reliably, the vulnerabilities introduced in the cyber layer to measure, monitor, and control power systems will reduce the resilient operation.

Islanding is classified as a clustering problem within the context of graph theory [10]. Clustering a graph network is the process of identifying the list of edges (transmission lines) that can be disconnected to maintain minimal discrepancies among the connecting vertices (buses) [24]. This is usually achieved via assessing the correlation between vertices in a specific graph, and then, removing the edges having the least correlation values. Various methods have been used to evaluate the correlation within a graph network in terms of edge weights [9], [12], [25]. In electric power system studies, the following edge weight functions have been used:

1) Topology: $W_{i,j} = 1$, where $(i, j) \in \mathcal{E}$
2) Admittance: $W_{i,j} = Y_{i,j} = 1/Z_{i,j}$ where $Z_{i,j}$ is the line impedance between buses i and j.
3) Power flow: $W_{i,j} = (|P_{i,j}| + |P_{j,i}|)/2$ where $P_{i,j}$ is the real power flow from bus i and bus j.
4) Optimal Power flow: $W_{i,j} = (|P^*_{i,j}| + |P^*_{j,i}|)/2$ where $P^*_{i,j}$ is the real power flow from bus i and bus j based on solving the optimal power flow problem.

C. Resilience-based Clustering

Different edge weight functions can be used to evaluate the characteristics and properties of a specific graph. In power system graphical representation, the topology weight function measures pure connectivity of a network whereas admittance weight matrix reveals the strength of graph edges (electrical distances). Also, power flow and optimal power flow weights are used to measure the loading level of transmission lines. However, these weight functions do not capture the fragility of system components during an extreme event [24]. In resilience-based studies, edge weights can be calculated based on the probability of failure of system components [26]. The weight matrix can be represented as $W_{i,j} = 1 - f_{i,j}$ where $f_{i,j}$ is the failure probability of an edge connecting buses i and j, which can be computed using fragility curve models [27]. Despite the capability to capture the vulnerability level of system components, the resilience-based weight function does not account for the loadability characteristics of system components.

A proper weight function that captures both the fragility and loadability features of graph edges will provide a better clustering against severe events. Four weight functions are proposed by integrating the steady-state solution of power flow and optimal power flow with the fragility behavior of power system components due to cyber-induced failures, which are explained as follows.

1) Integrated power flow and component availability: $W_{i,j} = ((|P_{i,j}| + |P_{j,i}|)/2)(1 - f_{i,j})$. Each element in the weight matrix corresponds to the multiplication of the average power flow and the probability of success for the corresponding edge.
2) Integrated optimal power flow and component availability: $W_{i,j} = ((|P^*_{i,j}| + |P^*_{j,i}|)/2)(1 - f_{i,j})$. Each element in the weight matrix corresponds to the multiplication of the optimal real power flow and the probability of success for the corresponding edge.
3) Integrated normalized power flow and component unavailability: $W_{i,j} = ((|\hat{P}_{i,j}| + |\hat{P}_{j,i}|)/2)(f_{i,j})$, where $\hat{P}$ is the normalized power flow between i and j.
4) Integrated normalized optimal power flow and component unavailability: $W_{i,j} = ((|\hat{P}^*_{i,j}| + |\hat{P}^*_{j,i}|)/2)(f_{i,j})$, where $\hat{P}^*$ is the normalized optimal power flow between i and j.

The normalized power flow values are selected to map the loadability level of transmission lines on a scale from zero to one—higher values imply higher loadability. Also, this ensures that same priority is given to both probability of failure (fragility feature) and power flow (loadability feature), since both reside within the same range. The probability of failure of a physical component can be computed using the probability of failure of the corresponding communication link as described in [23] and summarized as follows.

$$f_{i,j} = \begin{cases} f^{ns}_{i,j} & \text{if node channel assigned to edge}(i,j) \text{ fails} \\ f^{s}_{i,j} & \text{if switch connected to edge}(i,j) \text{ fails} \\ f^{bs}_{i,j} & \text{if branch channel assigned to edge}(i,j) \text{ fails} \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

III. Spectral Clustering for Defensive Islanding

This section explains hierarchical spectral clustering method to create defensive islands. Also, it provides a brief description of the clustering evaluation criteria including minimal amount of load curtailment and radiality constraints.

A. Hierarchical Spectral Clustering

The concept of hierarchical spectral clustering has been introduced in [24] for transmission power systems and in [25] for distribution systems. The general idea is to split a graph network into K sub-graphs. First, the normalized Laplacian matrix L_n representing a specific graph is evaluated using (5).

$$L_n = I - D^{-1/2} W D^{-1/2}, \tag{5}$$

where I is identity matrix, W is the edge weight matrix, and D is the diagonal degree matrix, which can be calculated as follows.

$$D_{j,j} = \sum_{i=1}^{\mathcal{N}} W_{j,i}. \tag{6}$$

The formulated Laplacian matrix is used to determine the first K eigenvectors corresponding to the smallest eigenvalues. The extracted eignvectors represent the coordinates of the graph vertices in $\mathbb{R}^K$. Once the K coordinate vectors are computed, the edge distance between each graph vertex, $i \in \mathcal{N}$ and all $k \in K$ vertices is computed. A specific vertex i will be assigned to cluster k based on the minimum euclidean distance. In other words, the minimum distance over a path between i and k is used to allocate graph vertices into a specific cluster. Detailed illustration of the presented method can be found in [24].

B. Clustering Evaluation Criteria

Various methods have been used to assess the performance of the clustering techniques [28]. The evaluation criteria vary based on the system being assessed, the size of the graph, and the required objectives. In this paper, two criteria are selected to evaluate the validity and efficiency of the calculated clusters, which are explained below.

1) Minimal Amount of Load Curtailment

The minimal amount of load curtailment is an index that can be used to evaluate the level of resilience enhancement. The critical load curtailment can capture the severity of the multiple line outages due to a cyber-induced failure and is directly affected by the topology and locations of distributed energy resources (DERs) in a distribution system. The total load curtailment in a distribution network can be expressed as follows.

$$LC_{tot} = \sum_{i=1}^{\mathcal{N}} \Delta P_i, \tag{7}$$

where ΔP_i is the load curtailment at node i, and $\mathcal{N}$ is the total number of nodes in the system.

2) Radiality Constraints

Radiality requirements should be satisfied in distribution systems to align with the existing protection coordination schemes and voltage regulation fundamentals. Each cluster (microgrid) is represented by sub-graph $\mathcal{G}_k = (\mathcal{N}_k, \mathcal{E}_k)$, where $\mathcal{N}_k$ is a set of nodes (or vertices) and $\mathcal{E}_k$ is a set of edges (or branches) in the sub-graph or cluster. A node-branch incidence matrix A can be constructed using (8) for each cluster, such that $A \in \mathbb{R}^{n \times e}$, where $n = |\mathcal{N}_k|$ denotes the number of nodes and $e = |\mathcal{E}_k|$ denotes the number of edges of a particular cluster. Radialty constraint is satisfied if matrix A is a full rank matrix.

$$a_{i,j} = \begin{cases} +1 & \text{if branch } j \text{ starts at node } i \\ -1 & \text{if branch } j \text{ ends at node } i \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

C. Integrated Algorithm

Algorithm 1 provides the process of defensive islanding to split a distribution system into smaller grids considering the role of cyber-induced failures.

IV. Implementation and Results

The proposed approach is applied on a modified version of the 33-node distribution feeder for validation. The defensive islanding framework is formulated using hierarchical spectral clustering integrated with resilience-based weighting functions.

A. Data Description

A CPPS representing a modified version of the 33-node distribution feeder [29], [30] is formed, as shown in Fig. 1. Each power system node and transmission line is assigned to a specific communication switch as provided in Table I. These routers are responsible for receiving measurement signals and sending control signals to the assigned physical components. All communication switches are connected to the main control center. A compromised router implies potential failure of all communication signals to the assigned physical components. Though the communication topology plays a vital role in addressing the correlation between cyber failures, this paper focuses on the impact of cyber failures on the performance of power system components. To create independent microgrids, eight DERs are connected to the distribution feeder at arbitrarily chosen locations as shown in Fig. 1. The maximum power capacity of each DER is 500 kW. The proposed algorithm takes into consideration the DER locations in assigning proper islands. In this paper, it is required to determine proper islands based on predefined system resources and characteristics.

Algorithm 1: Overview of Defensive Islanding Considering Cyber-induced Failures

```
Input: Define physical layer graph ($\mathcal{G}_{\mathcal{P}}$), cyber layer
       graph ($\mathcal{G}_{\mathcal{C}}$), number of clusters ($K$), and
       clustering strategies ($S$)
Generate a cyber failure scenario
Solve the power flow and optimal power flow
Propagate the cyber-induced failure to the physical
  layer using (1), (2), and (3)
Evaluate the probability of failure of power
  components using (4)
for $s \leftarrow 1$ to $S$ do
    Compute the weight matrix $W$
    Calculate the Laplacian matrix $L_n$
    Evaluate the eigenvectors $K$
    Obtain clusters using hierarchical spectral
      methodology
    Remove lines (edges) to split the system into
      islands
    Calculate the minimal amount of load curtailment
      and radiality rank
Output: Defensive islands and their corresponding
        load curtailment and radiality rank
```

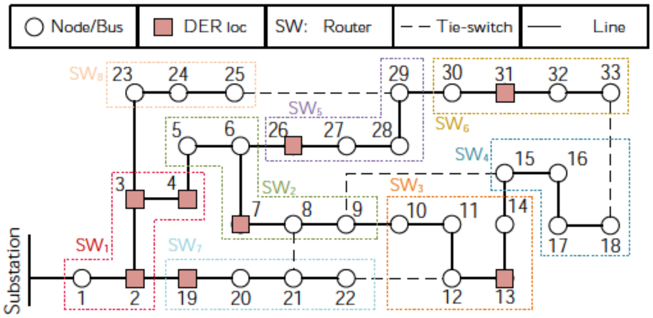

Fig. 1. CPPS schematic diagram of a modified 33-node distribution feeder

The proposed clustering approach relies mainly on the probability of failure of cyber failures during extreme events. Due to the lack of information regarding the failure behavior of cyber and communication components, several studies have adopted a scaling approach to compensate for the elevated extreme fragility conditions during severe conditions [31], [32]. In this work, the failure rate and repair time of the cyber components are adopted from [22], [23]. The failure rate of

TABLE I
ASSIGNED PHYSICAL COMPONENTS TO COMMUNICATION SWITCHES

Switch	Assigned Nodes	Assigned lines
SW_1	1,2,3,4	1,2,3,14,18,22
SW_2	5,6,7,8,9	5,6,7,8,9,25,33,34
SW_3	10,11,12,13,14	10,11,12,13,14,35
SW_4	15,16,17,18	15,16,17,36
SW_5	26,27,28,29	26,27,28,29,37
SW_6	30,31,32,33	30,31,32
SW_7	19,20,21,22	19,20,21
SW_8	23,24,25	23,24

the cyber components are scaled by a factor of four; whereas, the repair time is doubled from [30], [31].

B. Case Studies

Several test cases are conducted to validate the effectiveness of the proposed approach to provide defensive islanding for enhanced resilience. First, the proposed algorithm is tested for a predefined cyber failure scenario to ensure the robustness of the obtained islands. In this paper, we have used eight strategies for clustering the distribution system as shown in Table II. Two criteria are used for comparison: the minimal amount of load curtailment and the radiality constraints. A clustering strategy resulting in small amount of load curtailment and satisfied radiality constraints is preferred. In the second case, the robustness of the proposed algorithm against diverse cyber failure scenarios is validated. Finally, the third case provides a deeper analysis on the trade-off between sizes of clusters and efficiency of the proposed algorithm.

TABLE II
CLUSTERING STRATEGIES

Index	Weight matrix
S_1	Admittance
S_2	Power flow
S_3	Optimal power flow
S_4	Resilience-based
S_5	Integrated power flow and component availability
S_6	Integrated optimal power flow and component availability
S_7	Integrated power flow and component unavailability
S_8	Integrated optimal power flow and component unavailability

1) Algorithm Validation:

In this case, a predefined cyber-induced failure is simulated. The impact of the cyber failure is propagated to the physical system using the coupling matrices described in section II-A. The communication router SW_7 is assumed to be compromised resulting in a severe potential physical failure of 3 line segments and 4 load nodes. The probability of failure of physical components is computed based on the conditional probability failure of a connected cyber link as explained in section III-A. For fair comparison, all clustering strategies are set to split the distribution feeder into four independent islands.

Fig. 2 shows the clusters obtained for each strategy represented by different colors. The number of nodes in each cluster varies from one strategy to another. For instance, S_2 and S_5 have two islands each composed of a single node (7 and 19) which undermines these strategies to provide less resilient microgrids. In other words, nodes 7 and 19 could have been connected to nearby nodes yielding enhanced resilient topology. Strategies S_7 and S_8 provide very similar clustering solutions; however, the difference relies in the capability of S_8 to capture the whole generation benefits of the existing DERs. In S_4, the clusters are formed based on the resilience level of system components. This results in islands that do not follow radiality constraints and ignore system operating conditions such as cluster C_1 including node 7 and 20.

Table III shows the amount of load curtailment (LC) and degree of radiality (R) of all clusters obtained by different strategies. The R value reflects the number of clusters satisfying radiality constraints within a specific clustering strategy. It is obvious that the proposed strategies (S_7 and S_8) result in least amount of load curtailment relative to other clustering strategies with only 13% of the system nominal load to be curtailed. In general, using steady-state value of admittance matrix (S_1) and power flow solution (S_2) is not sufficient for proper clustering, specifically during severe conditions. Also, using resilience-based clustering (S_4) solely results in much higher curtailment as it ignores the loadability behavior of distribution line segments. Though S_3 provides acceptable results compared to S_5 and S_6, the obtained solution relies on the performance of the system prior to a cyber-induced failure ignoring the fragility behavior of each system component. On the other hand, the effectiveness of the proposed algorithm to provide clusters satisfying radiality constraints has been confirmed through values of R. Both S_7 and S_8 show that all obtained clusters satisfy the radial topology configuration of a distribution system. Also, it is noticeable that S_2, S_4, and S_5 do not usually maintain radial topology in the formed islands.

TABLE III
LOAD CURTAILMENT AND RADIALITY RANK OF CLUSTERING STRATEGIES

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
LC (MW)	1.635	1.545	1.125	1.755	1.545	1.125	0.910	0.470
LC (%)	44	42	30	47	42	30	25	13
R	3	2	3	2	2	3	4	4

2) Assessing Stochastic Behavior of Cyber Failures:

The solution of the proposed strategy will vary based on the cyber-induced failure scenario. In this case, the efficiency of the proposed clustering approach is validated under different cyber failure scenarios. A total of 10,000 cyber failure scenarios with diverse impact level are randomly generated and simulated. The amount of load curtailment and radiality rank are computed for each failure scenario. All clustering strategies are required to split the system into four independent islands.

Table IV summarizes the main statistical parameters including the average, the standard deviation, the minimum value, and the maximum value of the load curtailment and

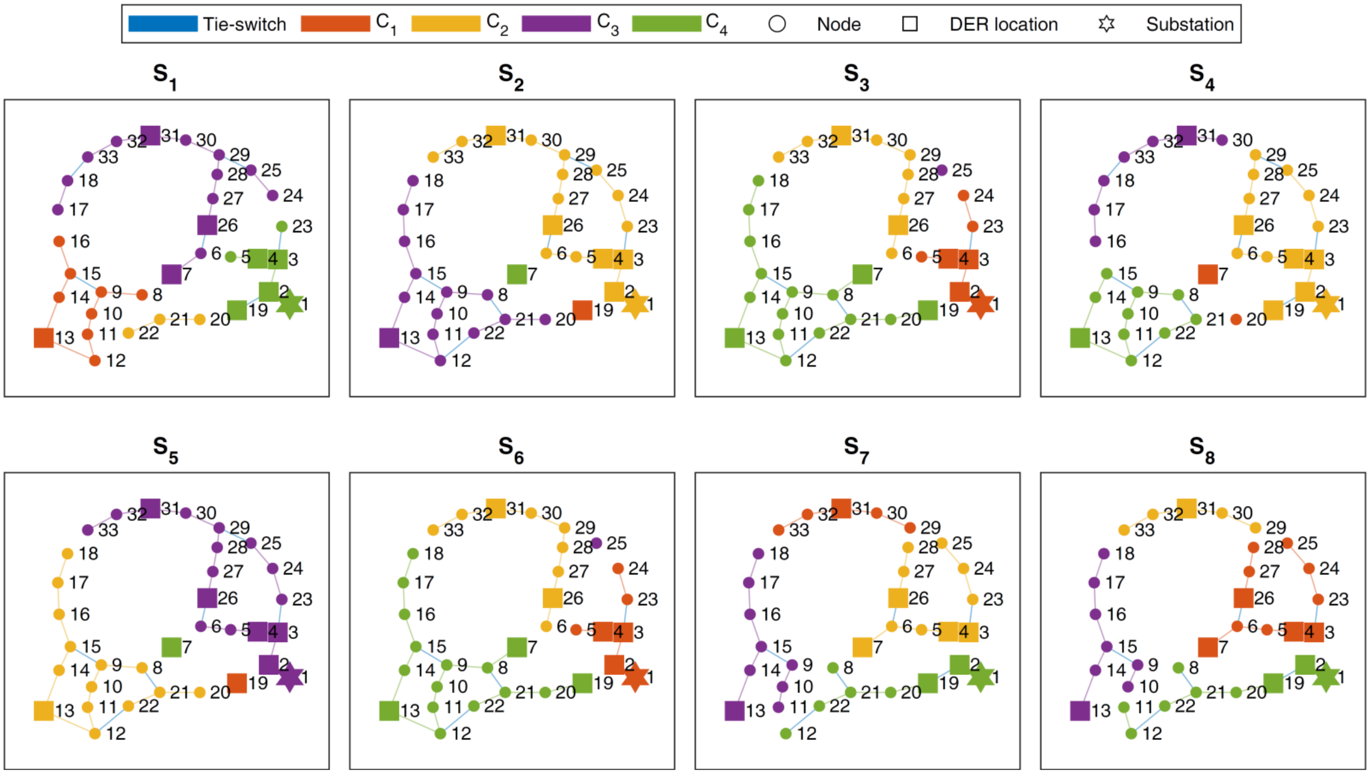

Fig. 2. Clusters using different strategies

radiality rank for all the clustering strategies. Strategies S_1, S_2, and S_3 provide the same amount of load curtailment regardless the simulated cyber failure scenario because these strategies rely mainly on the steady-state constant system characteristics and power flow in the system. Based on the load curtailment, S_8 shows the least average load curtailments which confirms its effectiveness to cluster the distribution system into islands considering both the loadability of distribution lines and the vulnerability of system components. Also, S_6 and S_7 provide acceptable values compared to basic clustering strategies (S_1, S_2, and S_3). As previously noted, the resilience-based clustering does not usually provide the best solution given diverse system operational conditions. The wide spectrum of load curtailment value realized in S_7 and S_8 ensures the capability of the proposed algorithm to capture the stochastic behavior of cyber failures. From the radiality prospective, it is noticeable that the average value of radiality rank of S_7 and S_8 exceeds three implying the tendency of the proposed strategies to maintain radiality constraints. Though S_1, S_2, and S_3 provide more robust results, one out the four clusters will always fail to satisfy the radiality constraints. In S_8, 32% of the simulated cases satisfy the radiality constraints. In general, the proposed clustering strategies outperform other strategies providing a clustering methodology that reduces the impact of cyber-induced failures on the performance of the power system.

TABLE IV
ASSESSMENT OF CLUSTERING STRATEGIES CONSIDERING CYBER-FAILURE UNCERTAINTIES

		S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
LC(MW)	mean	1.635	1.545	1.125	1.468	1.492	1.106	1.025	0.863
	st. dev.	0.0	0.0	0.0	0.246	0.180	0.166	0.377	0.398
	min	1.635	1.545	1.125	0.175	0.210	0.060	0.0	0.0
	max	1.635	1.545	1.125	1.935	1.935	1.935	2.195	2.015
R	mean	3.0	3.0	3.0	2.988	3.001	3.000	3.189	3.303
	st. dev.	0.0	0.0	0.0	0.108	0.028	0.025	0.459	0.495
	min	3	3	3	2	3	2	2	2
	max	3	3	3	3	3	4	4	4

3) Trade-off between Efficiency and Number of Clusters:

In this case, the effectiveness of the proposed clustering strategies to capture the impact of cyber-induced failures to create defensive islands is assessed based on the number of clusters. The same previously generated 10,000 cyber-induced failure scenarios are simulated for different number of clusters. The average load curtailment and the radiality rank are recorded for each specific number of clusters. Three strategies are selected for comparison including S_3, S_7, and S_8.

Fig. 3 shows the average value of both the load curtailment and the radiality rank. It is noticeable that the amount of load curtailment increases with the increase in the number of clusters. This reveals the importance of installing more DERs for better performance; however, the scope of this work is comparing the clustering strategies based on predefined energy resources. Strategy S_8 outperforms S_3 when having up to five clusters resulting in a better clustering strategy that encounters the cyber-induced failure. In case of six clusters formation, both S_3 and S_8 have very similar values of average load curtailment. Also, the performance of S_7 decreases as the number of cluster increases which can be inferred from the increase in amount of load curtailment relative to other strategies. Using the radiality rank criterion, the performance of the selected strategies is almost the same for small number of clusters. The higher the radiality rank is, the better the clustering strategy will be for a fixed number of clusters. Strategy S_8 outperforms S_3 and S_7 for the studied number of clusters. The performance of the proposed strategies is significantly impacted by the number DERs, the size of the system being analyzed, and the system physical characteristics. In general, the proposed strategies can be used to create defensive islands that capture the impact of cyber-induced failures into power systems.

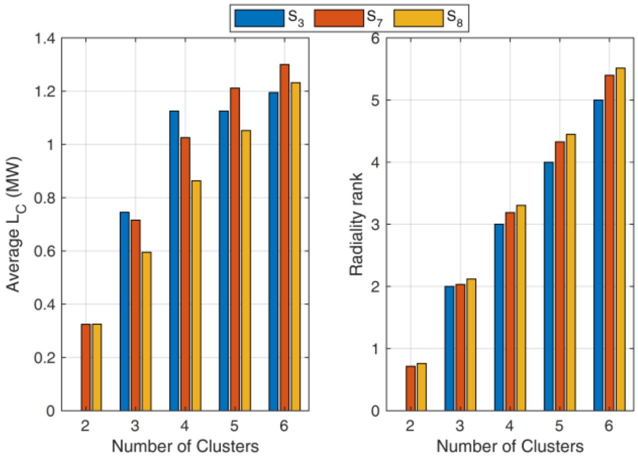

Fig. 3. Efficiency vs. cluster sizes

V. Conclusion

This paper has proposed a defensive islanding strategy for enhanced distribution system resilience against cyber-induced failures. The proposed method provides a list of islands considering both component fragility and system operating conditions. Hierarchical spectral clustering method was adapted to split the power system into specific number of independent microgrids. The minimal amount of load curtailment and radiality constraints were used to evaluate the performance of different clustering strategies. The methodology was tested on a CPPS representing a modified version of the the 33-node distribution feeder. The results showed the effectiveness of the proposed clustering strategies to provide a list of islands considering operating conditions of the system, the available generation resources, and the probability of failure of system components. Also, the robustness of the proposed framework against diverse cyber-induced failures was validated. The proposed algorithm provides system operators with a proactive resilience enhancement strategy to create defensive islands prior to an extreme or disruptive event.

Acknowledgement

This work was supported by the U.S. National Science Foundation (NSF) under Grant NSF 1847578.

References

[1] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (cpps): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151 019–151 064, 2020.

[2] B. Ti, G. Li, M. Zhou, and J. Wang, "Resilience assessment and improvement for cyber-physical power systems under typhoon disasters," *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 783–794, 2022.

[3] G. Cao, W. Gu, P. Li, W. Sheng, K. Liu, L. Sun, Z. Cao, and J. Pan, "Operational risk evaluation of active distribution networks considering cyber contingencies," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 3849–3861, 2020.

[4] E. L. Hotchkiss and A. Dane, "Resilience roadmap: a collaborative approach to multi-jurisdictional resilience planning," National Renewable Energy Lab.(NREL), Golden, CO (United States), Tech. Rep., 2019.

[5] S. Paul, F. Ding, K. Utkarsh, W. Liu, M. J. O'Malley, and J. Barnett, "On vulnerability and resilience of cyber-physical power systems: A review," *IEEE Systems Journal*, pp. 1–12, 2021.

[6] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, pp. 1–29, 2016.

[7] R. He, H. Xie, J. Deng, T. Feng, L. L. Lai, and M. Shahidehpour, "Reliability modeling and assessment of cyber space in cyber-physical power systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3763–3773, 2020.

[8] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1367–1388, 2017.

[9] R. Rocchetta, "Enhancing the resilience of critical infrastructures: Statistical analysis of power grid spectral clustering and post-contingency vulnerability metrics," *Renewable and Sustainable Energy Reviews*, vol. 159, p. 112185, 2022.

[10] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Boosting the power grid resilience to extreme weather events using defensive islanding," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2913–2922, 2016.

[11] M. Dabbaghjamanesh, B. Wang, A. Kavousi-Fard, S. Mehraeen, N. D. Hatziargyriou, D. N. Trakas, and F. Ferdowsi, "A novel two-stage multi-layer constrained spectral clustering strategy for intentional islanding of power grids," *IEEE Transactions on Power Delivery*, vol. 35, no. 2, pp. 560–570, 2020.

[12] J. Wu, X. Chen, S. Badakhshan, J. Zhang, and P. Wang, "Spectral graph clustering for intentional islanding operations in resilient hybrid energy systems," *arXiv preprint arXiv:2203.06579*, 2022.

[13] K. S. A. Sedzro, A. J. Lamadrid, and L. F. Zuluaga, "Allocation of resources using a microgrid formation approach for resilient electric grids," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 2633–2643, 2018.

[14] S. Xu, Y. Xia, and H.-L. Shen, "Analysis of malware-induced cyber attacks in cyber-physical power systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 12, pp. 3482–3486, 2020.

[15] W. Wang, A. Cammi, F. Di Maio, S. Lorenzi, and E. Zio, "A monte carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants," *Reliability Engineering & System Safety*, vol. 175, pp. 24–37, 2018.

[16] Y. Hayel and Q. Zhu, "Resilient and secure network design for cyber attack-induced cascading link failures in critical infrastructures," in *2015 49th Annual Conference on Information Sciences and Systems (CISS)*, 2015, pp. 1–3.

[17] A. Chaves, M. Rice, S. Dunlap, and J. Pecarina, "Improving the cyber resilience of industrial control systems," *International Journal of Critical Infrastructure Protection*, vol. 17, pp. 30–48, 2017.

[18] C. Li, "Securing us critical infrastructure against cyberattacks," in *Harvard model congress*, 2022.

[19] S. Slaughter, "Cybersecurity considerations impacting the us critical infrastructure: An overview," 2022.

[20] H. Lei and C. Singh, "Non-sequential monte carlo simulation for cyber-induced dependent failures in composite power system reliability evaluation," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1064–1072, 2017.

[21] H. Yuan, G. Li, Z. Bie, and M. Arif, "Distribution system reliability assessment considering cyber-physical integration," *Energy procedia*, vol. 158, pp. 2655–2662, 2019.

[22] Y. Han, Y. Wen, C. Guo, and H. Huang, "Incorporating cyber layer failures in composite power system reliability evaluations," *Energies*, vol. 8, no. 9, pp. 9064–9086, 2015.

[23] W. Liu, Q. Gong, H. Han, Z. Wang, and L. Wang, "Reliability modeling and evaluation of active cyber physical distribution system," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 7096–7108, 2018.

[24] R. J. Sánchez-García, M. Fennelly, S. Norris, N. Wright, G. Niblo, J. Brodzki, and J. W. Bialek, "Hierarchical spectral clustering of power grids," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2229–2237, 2014.

[25] S. Hasanvand, M. Nayeripour, S. A. Arefifar, and H. Fallahzadeh-Abarghouei, "Spectral clustering for designing robust and reliable multi-mg smart distribution systems," *IET Generation, Transmission & Distribution*, vol. 12, no. 6, pp. 1359–1365, 2018.

[26] S. Poudel and A. Dubey, "Critical load restoration using distributed energy resources for resilient power distribution system," *IEEE Transactions on Power Systems*, vol. 34, no. 1, pp. 52–63, 2019.

[27] M. Panteli and P. Mancarella, "The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience," *IEEE Power and Energy Magazine*, vol. 13, no. 3, pp. 58–66, 2015.

[28] A. Ng, M. Jordan, and Y. Weiss, "On spectral clustering: Analysis and an algorithm," *Advances in neural information processing systems*, vol. 14, 2001.

[29] Distribution System Analysis Subcommittee, "1992 test feeder cases," IEEE, PES, Tech. Rep., 1992. [Online]. Available: http://sites.ieee.org/pestestfeeders/resources/

[30] W. Liu, Y. Chen, L. Wang, N. Liu, H. Xu, and Z. Liu, "An integrated planning approach for distributed generation interconnection in cyber physical active distribution systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 541–554, 2020.

[31] A. Hussain, A. Oulis Rousis, I. Konstantelos, G. Strbac, J. Jeon, and H. Kim, "Impact of uncertainties on resilient operation of microgrids: A data-driven approach," *IEEE Access*, vol. 7, pp. 14 924–14 937, Jan. 2019.

[32] G. Li, P. Zhang, P. B. Luh, W. Li, Z. Bie, C. Serna, and Z. Zhao, "Risk analysis for distribution systems in the northeast u.s. under wind storms," *IEEE Trans. on Power Systems*, vol. 29, no. 2, pp. 889–898, 2014.